EXPERT INSIGHT

Mastering Blockchain

Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3

Fourth Edition

Imran Bashir

packt

Mastering Blockchain

Fourth Edition

Inner workings of blockchain, from cryptography and decentralized identities, to DeFi, NFTs and Web3

Imran Bashir

packt

BIRMINGHAM—MUMBAI

Mastering Blockchain

Fourth Edition

Copyright © 2023 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Senior Publishing Product Manager: Devika Battike
Acquisition Editor – Peer Reviews: Gaurav Gavas
Project Editor: Meenakshi Vijay
Content Development Editor: Rebecca Robinson
Copy Editor: Safis Editing
Technical Editor: Karan Sonawane
Proofreader: Safis Editing
Indexer: Manju Arasan
Presentation Designer: Rajesh Shirsath
Developer Relations Marketing Executive: Vidhi Vashisth

First published: March 2017
Second edition: March 2018
Third edition: August 2020
Fourth edition: March 2023

Production reference: 2040723

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.
ISBN: 978-1-80324-106-7

`www.packt.com`

Disclaimer: The information and viewpoints expressed in this book are those of the author and not necessarily those of any of the author's employers or their affiliates.

This book is dedicated with immeasurable love and gratitude to my beloved father.
The most affectionate, selfless, and hardworking man, who sacrificed everything for me.

> *Don’t worry, my son! Adversities come and go.*
>
> *—Scientist Bashir Ahmed Khan*

76 → 363 → 1245 → 1003 → 275 → 77 → 60 → 588 → 1 → 12 → 12 → 2215 → ∞

Contributors

About the author

Imran Bashir has an MSc in Information Security from Royal Holloway, University of London. He has a background in software development, solution architecture, infrastructure management, information security, and IT service management. His current focus is on the latest technologies, such as blockchain and quantum computing. He is a member of the Institute of Electrical and Electronics Engineers (IEEE). He has worked in various senior technology roles for different organizations around the world.

I would like to thank Edward Doxey for his dedication and Packt for their support and guidance throughout this project. I also want to thank John Cornyn, who read the previous edition of this book and suggested some corrections, as well as the reviewers of this edition.

I want to thank my wife and children for their support while I was writing, especially during the time I was supposed to spend with them.

Finally, I want to thank my father, who has always been there for me and always will be. And my mother, whose encouragement makes difficult obstacles easy to surmount for me. My parents' prayers and unconditional love for me have enabled me to achieve anything I desire.

Disclaimer: The information and viewpoints expressed in this book are those of the author and not necessarily those of any of the author's employers or their affiliates.

About the reviewers

Brian Wu is a senior blockchain architect and consultant. Brian has over 20 years of hands-on experience across various technologies, including blockchain, big data, cloud, AI, systems, and infrastructure. He has worked on more than 50 projects in his career.

He has written nine books, published by O'Reilly, Packt, and Apress, on popular fields within the blockchain domain, including *Learn Ethereum, First Edition*; *Learn Ethereum, Second Edition*; *Blockchain for Teens*; *Hands-On Smart Contract Development with Hyperledger Fabric V2*; *Hyperledger Cookbook*; *Blockchain Quick Start Guide*; *Security Tokens and Stablecoins Quick Start Guide*; *Blockchain By Example*; and *Seven NoSQL Databases in a Week*.

Shailesh B. Nair is a computer engineer and has worked in software development for the last 21 years. He has been involved in blockchain development for about 8 years using different blockchain frameworks, like Ethereum (L1, L2, L3), Substrate, Polkadot, Solana, Cosmos (IBC), CasperLabs, Tezos, etc using various programming languages like C++, Rust, Golang, Ocaml, and Haskell.

He has worked with many different crypto startups since 2014 and as a blockchain consultant, he has worked with Mina Protocol, FTX, and others.

I would like to thank my friends who have worked with me on projects related to blockchain.

Join us on Discord!

To join the Discord community for this book – where you can share feedback, ask questions to the author, and learn about new releases – follow the QR code below:

`https://packt.link/ips2H`

Table of Contents

Preface xxvii

Chapter 1: Blockchain 101 1

The growth of blockchain technology 1

Progress towards maturity • 2

Rising interest • 3

Distributed systems 4

CAP theorem • 6

PACELC theorem • 8

The history of blockchain 8

Bitcoin • 9

Electronic cash • 9

Introducing blockchain 11

Blockchain architecture • 12

Blockchain by layers • 12

Blockchain in business • 14

Generic elements of a blockchain • 14

Blockchain functionality • 18

Benefits and features of blockchain • 20

Limitations of blockchain technology • 21

Types of blockchain 23

Distributed ledgers • 23

Shared ledger • 24

Public blockchains • 24

Private blockchains • 24

Semi-private blockchains • 24

Permissioned ledger • 25

Fully private and proprietary blockchains • 25
Tokenized blockchains • 25
Tokenless blockchains • 25
Layer 1 blockchains • 26
Monolithic and polylithic blockchains • 26
Layer 2 blockchains • 26
Sidechains • 26
Summary 27

Chapter 2: Decentralization 29

Introducing decentralization 29
Methods of decentralization • 33
Disintermediation • 33
Contest-driven decentralization • 34
Quantifying decentralization • 34
Benefits of decentralization • 36
Evaluating requirements • 37
Full-ecosystem decentralization 38
Storage • 38
Communication • 39
Computing power • 40
Decentralization in practice 42
Smart contracts • 42
Autonomous agents • 42
Decentralized organizations • 43
Decentralized autonomous organizations • 43
Decentralized autonomous corporations • 43
Decentralized autonomous societies • 44
Decentralized applications • 44
Criteria for a DApp • 46
Operations of a DApp • 46
Design of a DApp • 46
Innovative trends 48
Decentralized web • 48
Web 1 • 49
Web 2 • 49
Web 3 • 49
Summary 49

Chapter 3: Symmetric Cryptography 51

Introducing cryptography 52

Services provided by cryptography • 52

Cryptographic primitives 54

Keyless primitives • 55

Random numbers • 55

Hash functions • 56

Symmetric key primitives • 67

Message authentication codes • 68

Secret key ciphers • 69

Advanced Encryption Standard 74

Data Encryption Standard • 74

How AES works • 74

Encrypting and decrypting using AES • 76

Summary 77

Chapter 4: Asymmetric Cryptography 79

Foundational mathematics 79

Asymmetric cryptography 80

Public and private keys • 80

Asymmetric cryptography algorithms • 82

Integer factorization • 82

Discrete logarithm • 82

Elliptic curves • 83

Integrated encryption scheme • 83

Introducing RSA 83

Encrypting and decrypting with RSA • 85

Introducing ECC 87

Mathematics behind ECC • 87

Point addition • 88

Point doubling • 91

Point multiplication • 92

The discrete logarithm problem • 93

Generating keys with ECC • 95

Digital signatures 98

RSA digital signature algorithms • 98

Generating RSA digital signatures • 100

The elliptic curve digital signature algorithm • 100

Generating ECDSA digital signatures • 102

Different types of digital signatures • 104

Blind signatures • 104

Multisignatures • 105

Threshold signatures • 106

Aggregate signatures • 108

Ring signatures • 108

Cryptographic constructs and blockchain technology 109

Homomorphic encryption • 109

Secret sharing • 109

Commitment schemes • 110

Zero-knowledge proofs • 111

zk-SNARKs • 113

zk-STARKs • 115

Zero-knowledge range proofs • 116

Encoding schemes • 116

Base64 • 117

base58 • 117

Verifiable random functions • 117

Summary 118

Chapter 5: Consensus Algorithms 119

Introducing consensus 119

Fault tolerance • 120

FLP impossibility • 121

Analysis and design 122

Model • 122

Processes • 122

Timing assumptions • 123

Classification 123

Algorithms 124

CFT algorithms • 124

Paxos • 124

Raft • 127

BFT algorithms • 129

Practical Byzantine Fault Tolerance • 129

Istanbul Byzantine Fault Tolerance • 134

Tendermint • 137

Nakamoto consensus • 144

Variants of PoW • 146

HotStuff • 151

Choosing an algorithm 155

Finality • 155

Speed, performance, and scalability • 156

Summary 156

Chapter 6: Bitcoin Architecture 157

Introducing Bitcoin 157

Cryptographic keys 159

Private keys in Bitcoin • 159

Public keys in Bitcoin • 160

Addresses 161

Typical Bitcoin addresses • 161

Advanced Bitcoin addresses • 163

Transactions 163

Coinbase transactions • 164

The transaction lifecycle • 165

Transaction validation • 166

Transaction fees • 166

The transaction data structure • 167

Metadata • 169

Inputs • 169

Outputs • 170

Verification • 170

The Script language • 170

Opcodes • 171

Standard transaction scripts • 171

Contracts • 174

Transaction bugs • 175

Blockchain 176

Structure • 176

The genesis block • 178

Stale and orphan blocks • 179
Forks • 179
Properties • 180
Miners 181
Proof of Work (PoW) • 182
Mining systems • 184
CPU • 184
GPU • 184
FPGAs • 185
ASICs • 185
Mining pools • 186
Network 186
Types of messages • 187
Client software • 192
Bloom filters • 192
Wallets 194
Summary 196

Chapter 7: Bitcoin in Practice 197

Bitcoin in the real world 197
Bitcoin payments 198
Innovation in Bitcoin 200
Bitcoin improvement proposals • 201
Advanced protocols • 202
Segregated Witness • 202
Bitcoin Cash • 204
Bitcoin Unlimited • 205
Bitcoin Gold • 205
Taproot • 205
Extended protocols on top of Bitcoin • 206
Colored coins • 206
Counterparty • 207
Altcoins from Bitcoin • 208
Bitcoin client installation 209
Types of clients and tools • 209
Setting up a Bitcoin node • 210
Setting up the source code • 210

Setting up bitcoin.conf • 211
Starting up a node in the testnet • 211
Starting up a node in regtest • 212
Experimenting further with bitcoin-cli 214
Using the Bitcoin command-line tool • 216
Using the JSON-RPC interface • 217
Using the HTTP REST interface • 218
Bitcoin programming 219
Summary 219

Chapter 8: Smart Contracts 221

Introducing smart contracts 221
Definitions • 222
Properties • 222
Real-world application • 224
Ricardian contracts 225
Smart contract templates 229
Oracles 231
Software-and network-assisted proofs • 233
TLSNotary • 233
TLS-N-based mechanism • 233
Hardware device-assisted proofs • 234
Android proof • 234
Ledger proof • 234
Trusted hardware-assisted proofs • 235
Types of blockchain oracles • 236
Inbound oracles • 236
Outbound oracles • 238
Cryptoeconomic oracles • 239
Blockchain oracle services • 239
Deploying smart contracts 240
The DAO 241
Advances in smart contract technology 242
Solana Sealevel • 242
Digital Asset Modeling Language • 243
Summary 245

Chapter 9: Ethereum Architecture 247

Introducing Ethereum 247

Cryptocurrency 250

Keys and addresses 250

Accounts 254

Transactions and messages 255

MPTs • 256

Transaction components • 257

Recursive Length Prefix • 261

Gas • 262

Transaction types • 264

Simple transactions • 264

Contract creation transactions • 264

Message call transactions • 265

Messages • 265

Transaction validation and execution • 266

State and storage in the Ethereum blockchain • 267

The world state • 268

The account state • 268

Transaction receipts • 269

Ethereum virtual machine 270

Execution environment • 273

The machine state • 273

Blocks and blockchain 274

The genesis block • 276

Block validation, finalization, and processing • 276

Block difficulty mechanism • 278

Nodes and miners 279

The consensus mechanism • 279

Forks in the blockchain • 281

The Ethereum network 281

Main net • 282

Test nets • 282

Private nets • 282

Precompiled smart contracts 286

Programming languages • 287

Solidity • 287

Runtime bytecode • 288

Opcodes • 288

Wallets and client software **289**

Wallets • 289

Geth • 289

Light clients • 289

Supporting protocols **290**

Whisper • 290

Swarm • 290

Summary **292**

Chapter 10: Ethereum in Practice 293

Ethereum payments **294**

Innovations in Ethereum **295**

Difficulty time bomb • 295

EIP-1559 • 296

The merge and upcoming upgrades • 298

Programming with Geth **298**

Installing and configuring the Geth client • 299

Creating a Geth new account • 299

Querying the blockchain using Geth • 301

Geth console • 301

Geth attach • 301

Geth JSON RPC API • 302

Setting up a development environment **304**

Connecting to test networks • 305

Creating a private network • 305

Starting up the private network • 307

Experimenting with the Geth JavaScript console • 310

Mining and sending transactions • 312

Introducing Remix IDE **318**

Interacting with the Ethereum Blockchain with MetaMask **321**

Installing MetaMask • 321

Creating and funding an account with MetaMask • 322

Using MetaMask and Remix IDE to deploy a smart contract • 324

Adding a custom network to MetaMask and connecting it with Remix IDE • 325

Importing accounts into MetaMask using keystore files • 328
Deploying a contract with MetaMask • 331
Interacting with a contract through MetaMask using Remix IDE • 336
Summary 342

Chapter 11: Tools, Languages, and Frameworks for Ethereum Developers 343

Languages 344
The Solidity compiler 344
Installing solc • 344
Experimenting with solc • 345
Tools, libraries, and frameworks 347
Node.js • 347
Ganache • 348
ganache-cli • 348
Ganache UI • 349
Truffle • 351
Drizzle • 352
Other tools • 352
Contract development and deployment 353
Writing smart contracts • 353
Testing smart contracts • 353
Deploying smart contracts • 354
The Solidity language 354
Functions • 355
Variables • 359
Local variables • 359
Global variables • 359
State variables • 360
Data types • 361
Value types • 361
Reference types • 363
Control structures • 365
Events • 366
Inheritance • 367
Libraries • 367
Error handling • 368
Summary 369

Chapter 12: Web3 Development Using Ethereum 371

Interacting with contracts using Web3 and Geth 371

Deploying contracts • 372

Using solc to generate ABI and code • 376

Querying contracts with Geth • 377

Interacting with Geth using POST requests • 380

Interacting with contracts via frontends 381

Installing the web3.js JavaScript library • 382

Creating a web3 object • 383

Creating an app.js JavaScript file • 384

Creating a frontend webpage • 387

Calling contract functions • 388

Creating a frontend webpage • 389

Deploying and interacting with contracts using Truffle 391

Installing and initializing Truffle • 392

Compiling, testing, and migrating using Truffle • 393

Interacting with the contract • 398

Using Truffle to test and deploy smart contracts • 399

Deployment on decentralized storage using IPFS • 404

Summary 406

Chapter 13: The Merge and Beyond 407

Introduction 407

Ethereum after The Merge 408

The Beacon Chain • 409

Beacon nodes • 410

Consensus client • 411

Execution client • 411

Validator client • 411

Proof-of-stake • 415

P2P interface (networking) • 421

The Merge 422

Sharding 432

The future roadmap of Ethereum 440

Summary 441

Chapter 14: Hyperledger 443

Projects under Hyperledger 444

Distributed ledgers • 444

Fabric • 444

Sawtooth • 445

Iroha • 445

Indy • 446

Besu • 446

Libraries • 446

Aries • 446

Transact • 447

Ursa • 447

AnonCreds • 447

Tools • 447

Cello • 448

Caliper • 448

Domain-specific • 448

Grid • 448

Hyperledger reference architecture 449

Hyperledger design principles • 451

Hyperledger Fabric 452

Key concepts • 452

Membership service • 453

Blockchain services • 454

Smart contract services • 456

APIs and CLIs • 456

Components • 456

Peers/nodes • 457

Clients • 457

Channels • 457

World state database • 457

Private data collections • 458

Transactions • 458

Membership Service Provider • 458

Smart contracts • 459

Crypto service provider • 459

Applications • 459

Chaincode implementation • 460

The application model • 462

Consensus mechanism • 462

Transaction lifecycle • 463

Fabric 2.0 .... **465**

New chaincode lifecycle management • 465

New chaincode application patterns • 466

Summary **468**

Chapter 15: Tokenization 469

Tokenization on a blockchain **470**

Advantages of tokenization • 470

Disadvantages of tokenization • 472

Types of tokens **473**

Fungible tokens • 473

Non-fungible tokens • 473

Stable tokens • 474

Security tokens • 475

Process of tokenization **475**

Token offerings **476**

Initial coin offerings • 476

Security token offerings • 477

Initial exchange offerings • 477

Equity token offerings • 477

Decentralized autonomous initial coin offering • 478

Other token offerings • 478

Token standards **479**

ERC-20 • 479

ERC-223 • 480

ERC-777 • 480

ERC-721 • 480

ERC-884 • 480

ERC-1400 • 481

ERC-1404 • 481

ERC-1155 • 482

ERC-4626 • 482

Building an ERC-20 token 483

Building the Solidity contract • 483

Deploying the contract on the Remix JavaScript virtual machine • 488

Adding tokens in MetaMask • 493

Emerging concepts 495

Tokenomics/token economics • 495

Token engineering • 495

Token taxonomy • 496

Summary 496

Chapter 16: Enterprise Blockchain 497

Enterprise solutions and blockchain 498

Success factors • 499

Limiting factors • 500

Requirements 501

Privacy • 502

Performance • 502

Access governance • 503

Further requirements • 503

Compliance • 503

Interoperability • 504

Integration • 505

Ease of use • 505

Monitoring • 505

Secure off-chain computation • 505

Better tools • 506

Enterprise blockchain versus public blockchain 506

Enterprise blockchain architecture 507

Designing enterprise blockchain solutions 509

TOGAF • 510

Architecture development method (ADM) • 511

Blockchain in the cloud • 513

Currently available enterprise blockchains 515

Enterprise blockchain challenges 517

Interoperability • 517

Lack of standardization • 517

Compliance • 518

Business challenges • 518

VMware Blockchain 518

Components • 519

Consensus protocol • 519

Architecture • 520

VMware Blockchain for Ethereum • 522

Quorum 522

Architecture • 522

Nodes • 523

Privacy manager • 524

Cryptography • 525

Privacy • 525

Enclave encryption • 527

Transaction propagation to transaction managers • 527

Enclave decryption • 528

Access control with permissioning • 529

Performance • 531

Pluggable consensus • 531

Setting up a Quorum network with IBFT 532

Installing and running Quorum Wizard • 532

Running a private transaction • 535

Attaching Geth to nodes • 535

Viewing the transaction in Cakeshop • 538

Further investigation with Geth • 539

Other Quorum projects 542

Remix plugin • 542

Pluggable architecture • 542

Summary 543

Chapter 17: Scalability 545

What is scalability? 545

Blockchain trilemma • 546

Methods for improving scalability • 548

Layer 0 – multichain solutions • 549

Polkadot • 549

Layer 1 – on-chain scaling solutions • 551

Layer 2 – off-chain solutions • 555

Layer 2 • 555

Rollups • 559

Data validity • 560

Data availability • 560

How rollups work • 561

Types of rollups • 563

Optimistic rollups • 563

ZK-rollups • 564

Technologies used for building ZK-rollups • 566

ZK-ZK-rollups • 573

Optimistic rollups vs ZK-rollups • 573

Fraud and validity proof-based classification of rollups • 575

Example • 577

Layer 3 and beyond • 579

Summary 580

Chapter 18: Blockchain Privacy 583

Privacy 583

Anonymity • 584

Confidentiality • 584

Techniques to achieve privacy 585

Layer 0 • 586

Tor • 586

I2P • 586

Indistinguishability obfuscation • 586

Homomorphic encryption • 587

Secure multiparty computation • 587

Trusted hardware-assisted confidentiality • 587

Mixing protocols • 588

CoinSwap • 589

TumbleBit • 590

Dandelion • 590

Confidential transactions • 592

MimbleWimble • 592

Zkledger • 593

Attribute-based encryption • 593

Anonymous signatures • 593

Zether • 594

Privacy using Layer 2 protocols • 594

Privacy managers • 594

Privacy using zero-knowledge • 594

Cryptographic Commitments • 595

Zero-knowledge proofs • 597

Building ZK-SNARKs • 601

Example • 610

Summary **616**

Chapter 19: Blockchain Security 619

Security **619**

Blockchain layers and attacks **621**

Hardware layer • 622

Network layer • 623

Blockchain layer • 624

Attacks on transactions • 624

Transaction replay attacks • 625

Attacks on consensus protocols • 626

Double-spending • 627

Selfish mining • 627

Forking and chain reorganization • 627

Blockchain application layer • 628

Smart contract vulnerabilities • 628

DeFi attacks • 631

Interface layer • 631

Oracle attacks/oracle manipulation attacks • 632

Attacks on wallets • 632

Attacks on layer 2 blockchains **634**

Cryptography layer • 635

Attacking public key cryptography • 635

Attacking hash functions • 636

Key management-related vulnerabilities and attacks • 636

ZKP-related attacks • 637

Security analysis tools and mechanism **638**

Formal verification • 639

Formal verification of smart contracts • 640

Model checking • 641

Smart contract security • 644

Oyente • 645

Solgraph • 646

Threat modeling **646**

Regulation and compliance **649**

Summary **649**

Chapter 20: Decentralized Identity 651

Identity **651**

Digital identity **652**

Centralized identity model • 652

Federated identity model • 653

Decentralized identity model • 657

Self-sovereign identity • 658

Components of SSI • 659

Identity in Ethereum **672**

Identity in the world of Web3, DeFi, and Metaverse **672**

SSI-specific blockchain projects **675**

Hyperledger Indy, Aries, Ursa, and AnonCreds • 675

Other projects • 676

Some other initiatives • 676

Challenges **676**

Summary **677**

Chapter 21: Decentralized Finance 679

Introduction **679**

Financial markets **681**

Trading • 681

Exchanges • 682

Orders and order properties • 682

Order management and routing systems • 683

Components of a trade • 683

Trade lifecycle • 684

Applications of blockchain in finance **685**

Insurance • 685

Post-trade settlement • 685

Financial crime prevention • 686

Payments • 688

Decentralized finance **690**

Properties of DeFi • 691

DeFi layers • 692

DeFi primitives • 693

DeFi services • 694

Asset tokenization • 694

Decentralized exchanges • 695

Flash loans • 701

Derivatives • 702

Money streaming • 703

Yield farming • 703

Insurance • 704

Decentralized lending – lending and borrowing • 704

Benefits of DeFi • 707

Uniswap • 708

Swap the token • 708

Uniswap liquidity pool • 710

Summary **714**

Chapter 22: Blockchain Applications and What's Next 715

Use cases **715**

IoT • 716

IoT architecture **716**

The physical object layer • 718

The device layer • 718

The network layer • 718

The management layer • 718

The application layer • 718

Benefits of IoT and blockchain convergence • 719

Implementing blockchain-based IoT in practice **722**

Setting up Raspberry Pi • 723

Setting up the first node • 725

Setting up the Raspberry Pi node • 726

Installing Node.js • 727

Building the electronic circuit • 728

Developing and running a Solidity contract • 729
Government 735
Border control • 735
Elections • 737
Citizen identification • 737
Health 738
Media 739
Blockchain and AI 740
Some emerging trends 741
Some challenges 743
Summary 745
Index 747

Preface

The goal of this book is to teach the theory and practice of distributed ledger technology to anyone interested in learning this fascinating new subject. Anyone can benefit from this book, whether a seasoned technologist, student, business executive, or enthusiast. To this end, I aim to provide a comprehensive and in-depth reference of distributed ledger technology that serves the expert and is also accessible to beginners. I primarily focus on describing the core characteristics of blockchain so that readers can build a strong foundation on which to build further knowledge and expertise. The main topics include core blockchain principles, cryptography, consensus algorithms, distributed systems theory, and smart contracts. In addition, practical topics such as programming smart contracts in solidity, building blockchain networks, using blockchain development frameworks such as Truffle, and writing decentralized applications and descriptions constitute a significant part of this book. Moreover, many types of blockchains, related use cases, and cross-industry applications of blockchain technology are discussed in detail.

This book is a unique blend of theoretical principles and hands-on application. Readers will not only be able to understand the technical underpinnings of this technology, but they will also be able to write code for smart contracts and build blockchain networks. Practitioners can use this book as a reference, and it can also serve as a textbook for students wishing to learn this technology. Indeed, some institutions have adopted previous editions of this book as a primary textbook for their courses on blockchain technology.

This book has six new chapters on the latest topics in blockchain, including scalability, security, privacy, the Ethereum Merge, decentralized identity, and decentralized finance.

I hope that this work will serve well technologists, teachers, students, scientists, developers, business executives, and anyone who wants to learn this fascinating technology for many years to come.

Who this book is for

This book is for anyone who wants to understand blockchain technology in depth. It can also be used as a reference resource by developers who are developing applications for blockchain. It can also be used as a textbook for courses related to blockchain technology and cryptocurrencies, as well as being a learning resource for various examinations and certifications related to cryptocurrency and blockchain technology.

What this book covers

Chapter 1, Blockchain 101, introduces the basic concepts of distributed computing, which blockchain technology is based on. It also covers the history, definitions, features, types, and benefits of blockchains, along with various consensus mechanisms that are at the core of blockchain technology.

Chapter 2, Decentralization, covers the concept of decentralization and its relationship with blockchain technology. Various methods and platforms that can be used to decentralize a process or a system will also be introduced.

Chapter 3, Symmetric Cryptography, introduces the theoretical foundations of symmetric cryptography, which is necessary to understand how various security services such as confidentiality and integrity are provided.

Chapter 4, Asymmetric Cryptography, introduces concepts such as public and private keys, digital signatures, and hash functions with practical examples.

Chapter 5, Consensus Algorithms, covers the fundamentals of consensus algorithms and describes the design and inner workings of several consensus algorithms. It covers both traditional consensus protocols and blockchain consensus protocols.

Chapter 6, Bitcoin Architecture, covers Bitcoin, the first and largest blockchain. It introduces technical concepts related to Bitcoin cryptocurrency in detail.

Chapter 7, Bitcoin in Practice, covers the Bitcoin network, relevant protocols, and various Bitcoin wallets. Moreover, advanced protocols, Bitcoin trading, and payments are also introduced. Moreover, various Bitcoin clients and programming APIs that can be used to build Bitcoin applications are covered.

Chapter 8, Smart Contracts, provides an in-depth discussion on smart contracts. Topics such as the history, the definition of smart contracts, Ricardian contracts, Oracles, and the theoretical aspects of smart contracts are presented in this chapter.

Chapter 9, Ethereum Architecture, introduces the design and architecture of the Ethereum blockchain in detail. It covers various technical concepts related to the Ethereum blockchain and explains the underlying principles, features, and components of this platform in depth. Other topics covered are related to the Ethereum Virtual Machine, mining, and supporting protocols for Ethereum.

Chapter 10, Ethereum in Practice, covers the topics related to setting up private networks for Ethereum smart contract development and programming.

Chapter 11, Tools, Languages, and Frameworks for Ethereum Developers, provides a detailed practical introduction to the Solidity programming language and different relevant tools and frameworks that are used for Ethereum development.

Chapter 12, Web3 Development Using Ethereum, covers the development of decentralized applications and smart contracts using the Ethereum blockchain. A detailed introduction to the Web3 API is provided along with multiple practical examples and a final project.

Chapter 13, The Merge and Beyond, introduces the latest development in Ethereum, such as the Beacon Chain, sharding, and future upgrades.

Chapter 14, *Hyperledger*, presents a discussion about the Hyperledger project from the Linux Foundation, which includes different blockchain projects introduced by its members.

Chapter 15, *Tokenization*, introduces the topic of tokenization, stable coins, and other relevant ideas such as initial coin offerings and token development standards.

Chapter 16, *Enterprise Blockchain*, covers the use and application of blockchain technology in enterprise settings and covers DLT platforms such as Quorum.

Chapter 17, *Scalability*, is dedicated to a discussion of one of the challenges, that is, scalablity, faced by blockchain technology and how to address it. We focus on layer 2 solutions to address this problem, however, other solutions are also discussed.

Chapter 18, *Blockchain Privacy*, introduces the problem of lack of privacy in blockchains and explains various techniques to address this limitation. We cover solutions to achieve confidentiality and anonymity in blockchains using techniques such as ZK-SNARKs, mixers, and various other methods.

Chapter 19, Blockchain Security, introduces the various security challenges in blockchains and how to solve them. These include smart contract security, formal verification, security concerns, and best practices at each layer of the blockchain system.

Chapter 20, *Decentralized Identity*, covers one of the hottest topics in the blockchain world. Decentralized identity is a cornerstone of the Web3 ecosytem. In this chapter, we explore the methods, techniques, and ecosystems that underpin the Web3 and decentralized identity landscape.

Chapter 21, *Decentralized Finance*, covers the use and application of decentralized finance, its various aspects, the use cases of blockchain in fianance, and different DeFi protocols.

Chapter 22, *Blockchain Applications and What's Next*, provides a practical and detailed introduction to the applications of blockchain technology in fields other than cryptocurrency, including the Internet of Things, government, media, and finance. It is aimed at providing information about the current landscape, projects, and research efforts related to blockchain technology.

Chapter 23, *Alternative Blockchains*, introduces alternative blockchain solutions and platforms as bonus content that is available online. It covers technical details and features of alternative blockchains and relevant platforms. This is a online chapter and you can read about it at the following link: `https://packt.link/OceZK`.

To get the most out of this book

In order to get the most out of this book, some familiarity with computer science and basic knowledge of a programming language is desirable.

Download the example code files

The code bundle for the book is hosted on GitHub at `https://github.com/PacktPublishing/Mastering-Blockchain-Fourth-Edition`.

We also have other code bundles from our rich catalog of books and videos available at `https://github.com/PacktPublishing/`.

Check them out!

Download the color images

We provide a PDF file that has color images of the screenshots/diagrams used in this book. You can download it here: `https://packt.link/5y4vk`.

Conventions used

There are a number of text conventions used throughout this book.

`CodeInText`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. For example: “Tapscript also enables easier future soft fork upgrades by using the new `OP_SUCCESS` opcode.”

A block of code is set as follows:

```
function ()
{
    throw;
}
```

Any command-line input or output is written as follows:

```
"Please send 0.00033324 BTC to address 1JzouJCVmMQBmTcd8K4Y5BP36gEFNn1ZJ3".
```

Bold: Indicates a new term, an important word, or words that you see on the screen. For instance, words in menus or dialog boxes appear in the text like this. For example: “**ACCOUNTS & KEYS** provides options to configure balance and the number of accounts to generate.”

Warnings or important notes appear like this.

Tips and tricks appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: Email `feedback@packtpub.com` and mention the book’s title in the subject of your message. If you have questions about any aspect of this book, please email us at `questions@packtpub.com`.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you reported this to us. Please visit `http://www.packtpub.com/submit-errata`, click **Submit Errata**, and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packtpub.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `http://authors.packtpub.com`.

Share Your Thoughts

Once you've read *Mastering Blockchain - Fourth Edition*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere? Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below

`https://packt.link/free-ebook/9781803241067`

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly